



Communications Technology for Improved Aviation Security

May 2005

**B. Farroha, C. Resch, G. Stoneburner, G. Preziotti, *R. Nichols*
Johns Hopkins University Applied Physics Laboratory**



Outline

- Overview
- Potential Missions and Technical Challenges
- Security System Engineering
- Recommendations



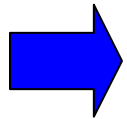
Overview

- Environment
 - Post-9/11 era and aviation security
 - Communications as an enabling technology
- Our paper:
 - Explores aviation security concepts that rely on communication systems technology such as:
 - Dissemination of on-board visual information
 - Other types of onboard sensor data distribution
 - Onboard audio monitoring and analysis
 - Data fusion multi-resources
 - Addresses a Communications Systems Engineering process for technology development
 - Presents a Security Systems Engineering process to assess/react to threats
 - Suggests areas for technical study



Outline

- Overview

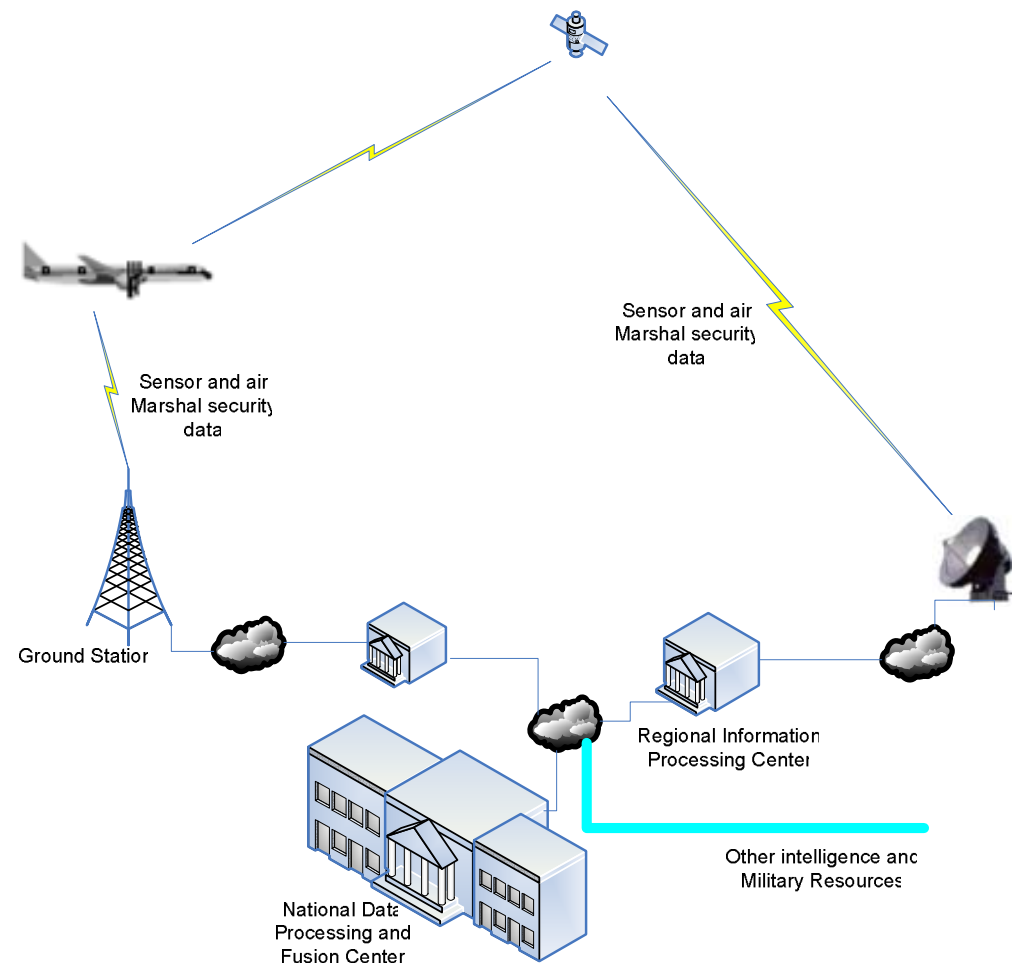


- Potential Missions and Technical Challenges
- Security System Engineering
- Recommendations



Air-to-Ground: Support for Sensor Downlinks

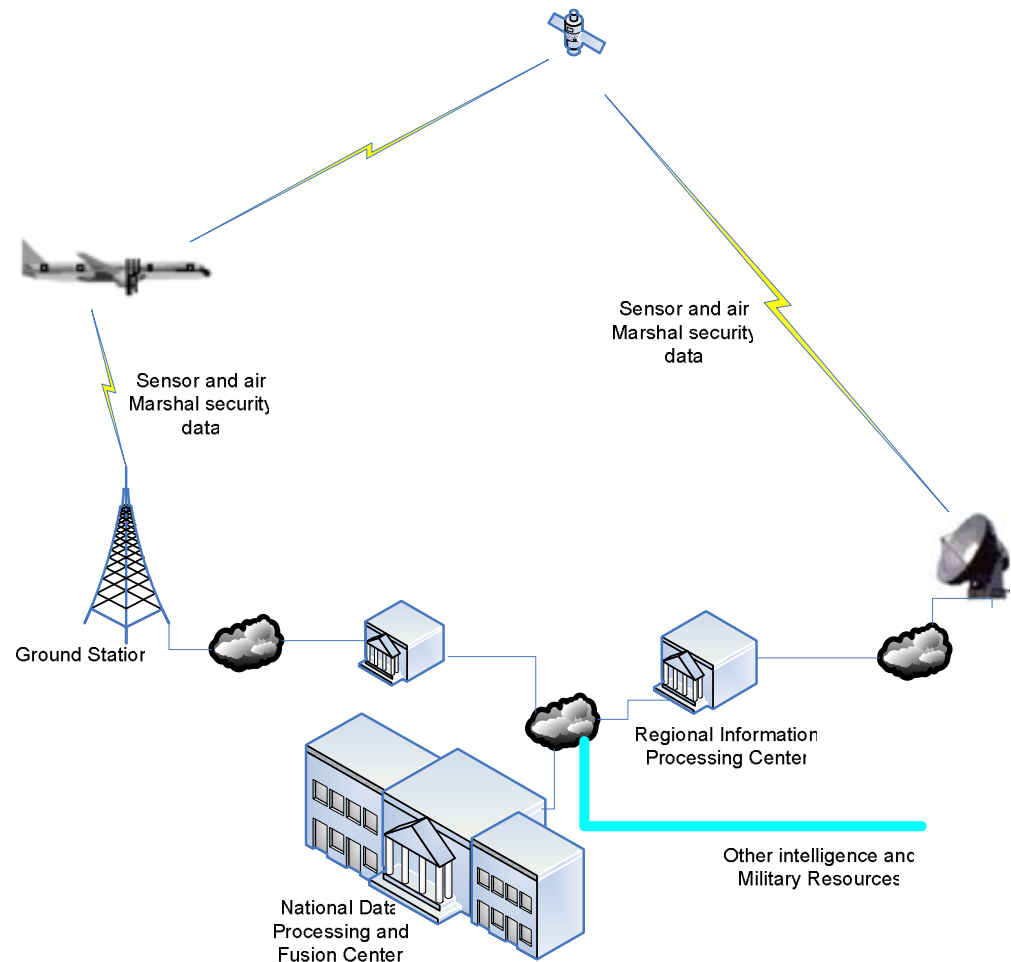
- Installation of passive sensors to send data such as:
 - Video/still images of cockpit and cabin
 - Information from chemical or biological sensors
 - Audio alerts via threshold levels
- Triggering alerts onboard aircraft via:
 - Sensor output
 - Observed actual situation development
 - Pilot or crew manual activation
 - Airport alert systems
 - Intelligence information





Air-to-Ground: Support for Air Marshals

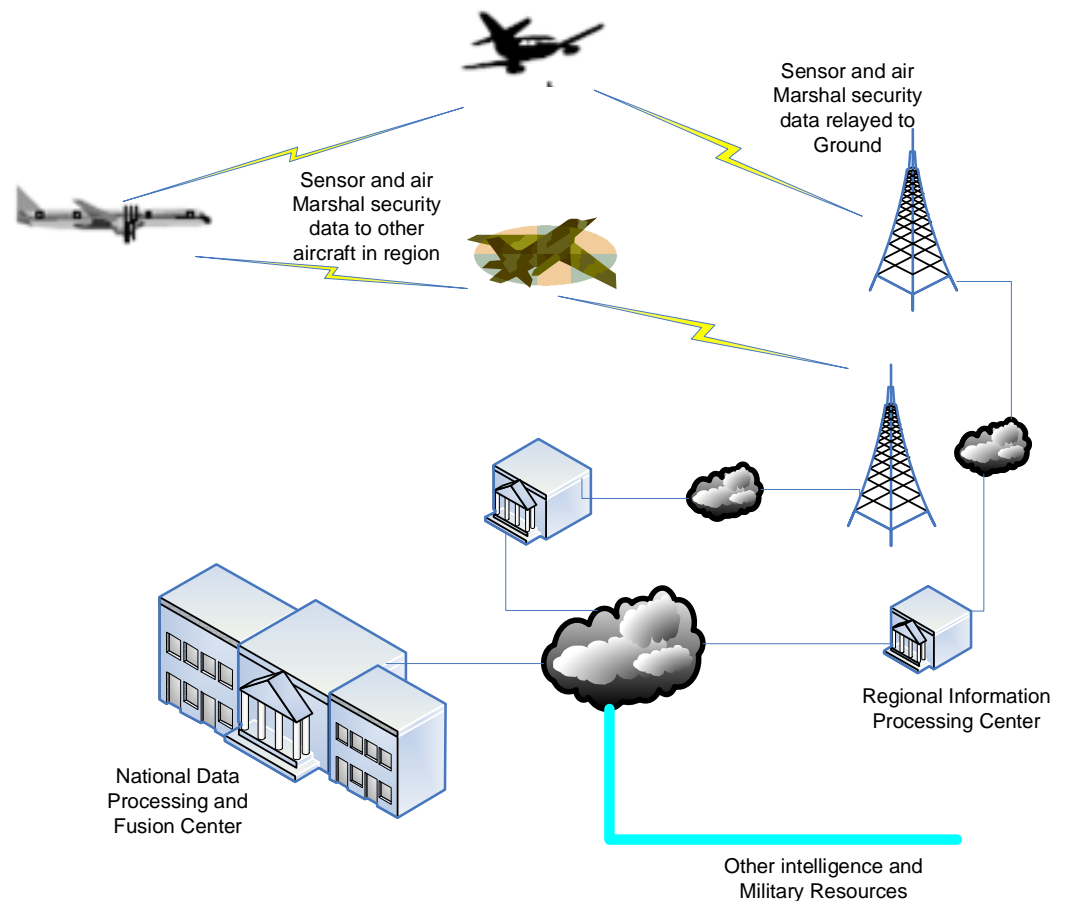
- Employ on-board communications for air marshals to communicate with ground
 - Status of flight
 - Passenger information
 - Coordination of activities
- Air-to-ground technical challenges
 - Use of existing frequencies/channels to communicate
 - Loading/prioritization on communications
 - Use of wireless devices to remotely connect anywhere on aircraft
 - Certification, cost, CONOPS





Air-to-Air Communications

- Air-to-air communications in the event of a crisis
 - With other civilian or military aircraft
 - To provide situational awareness so that action can be taken
 - Currently the existing infrastructure cannot support this capability
- Technical challenges:
 - Aircraft has limited space and power
 - Diverse aircraft means multiple configurations
 - Security of communications channels
 - Certification, cost, CONOPS





Comm. Systems Engineering Process

- Identify and quantify appropriate communications requirements
 - Performance
 - Legality
 - Safety
- Investigate existing air-to-ground and air-to-air communication systems
 - What are system capabilities?
 - Which systems are the most appropriate for this task?
 - What modifications may be required to them?
 - Potential technology gaps



- Capacity
- Latency
- Connectivity/topology
- Number of nodes
- Platform Constraints
- Coverage
- Link availability
- Integrity
- Cost
- Traffic type
- Security



Outline

- Overview
- Potential Missions and Technical Challenges
- ➡ • Security System Engineering
- Recommendations



Security System Engineering

- Methodology for Security Systems Engineering
 - Vital to ensure enhancements to aviation security are done correctly
 - Requires a rigorous approach to requirements analysis
 - Mandates a repeatable process from needs analysis through implementation
- Security Systems Engineering Process:
 - Define the organizational security policy
 - Define the system and its intended use
 - Categorize mission impact
 - Layout initial system
 - Assess risk
 - Determine security objectives and security controls



Categorize Mission Impact

- Three basic security needs
 - Confidentiality: Preserving authorized restrictions on information access and disclosure
 - Integrity: Guarding against improper information modification or destruction
 - Availability: Ensuring timely and reliable access to and use of information

Notional Mission Impact Matrix

Information	Confidentiality	Integrity	Availability
Air Traffic Control Information	High	High	High
Weather Information	Low	High	Medium
Maps	Medium	High	Medium
Flight Restriction Information	High	High	Medium
System Administration Information	High	High	Medium



Assess Risk



Unsophisticated

Example: Physical attack

Highly sophisticated

Example: Synchronized physical/electronic attack

***Need to conduct threat assessment
(continual process)***



Assess Risk (cont'd)

Notional Threat/Attack Matrix

Threats and Attacks Analysis		
Information	Threat-Source	Attack
Flight Restriction Information	Terrorists	Replay attack- cause flight restriction information to be inaccurate

Notional Risk Assessment Matrix

Risk Assessment						
Information	Threat-Source	Attack	Likelihood	Service Attacked	Impact	Risk
Flight restriction information	Terrorists	Replay	Medium	Integrity	High	Medium+High =High



Security Objectives and Controls

- Objectives provide strategy for how the risks will be addressed
- May be prevention, detection/response, or combination
- Security mechanisms must cover identified risks (one-to-one, one-to-many, many-to-one)

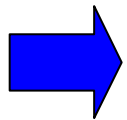
Notional Security Controls Matrix

Security Controls					
Information	Threat	Attack	Service Attacked	Risk	Control
Flight restriction information	Terrorists	Replay	Integrity	Medium+High =High	The information system shall protect the integrity of transmitted information. Cryptographic mechanisms will be employed to ensure recognition of changes during transmission



Outline

- Overview
- Potential Missions and Technical Challenges
- Security System Engineering

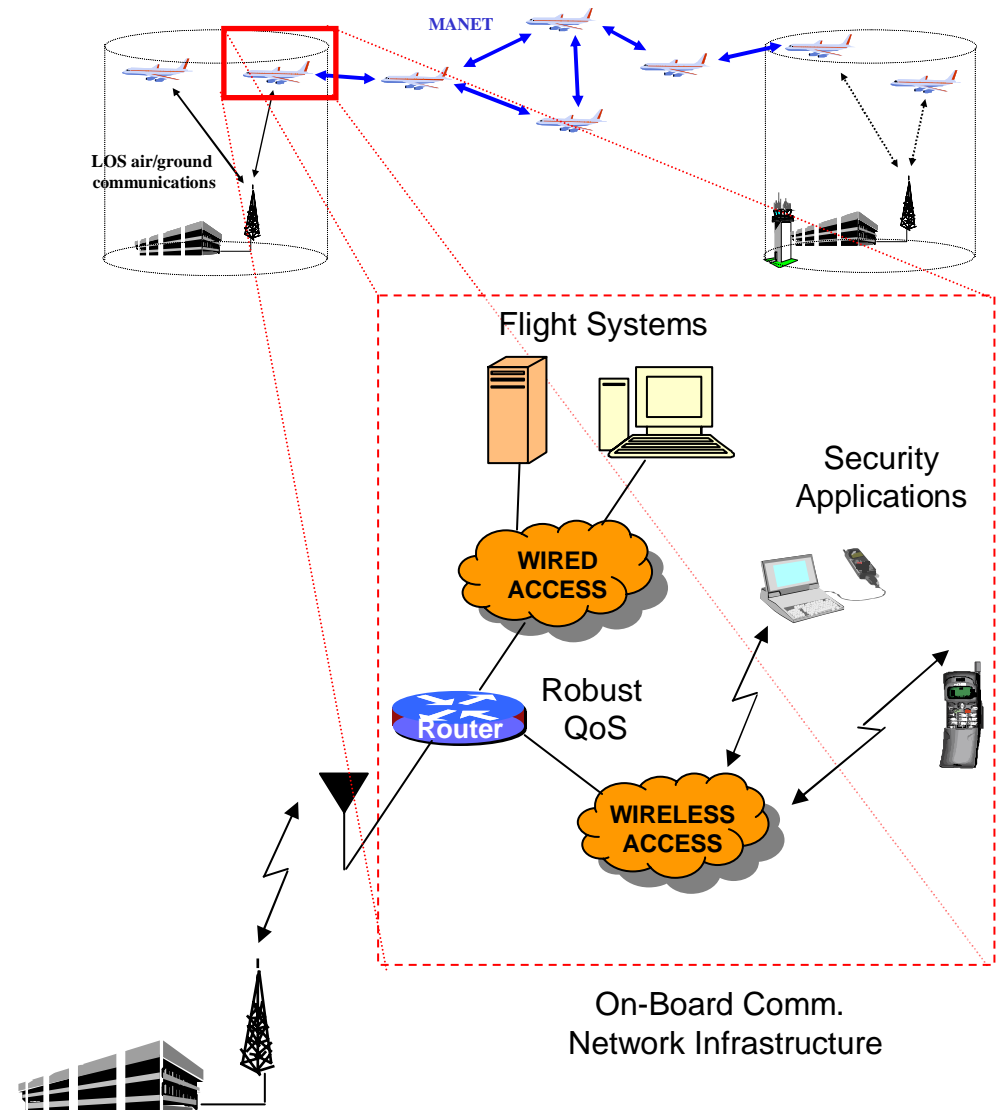


- Recommendations



Technology Gaps

- Technology gap analysis needs to be conducted
- Likely technology gaps:
 - Secure reconfiguration of communications assets
 - Intra- and inter- plane communications approaches and architectures
 - High capacity data links to the ground
 - Highly robust communications leveraging military investments (e.g. reconfigurable software radios)
 - Leveraging and enhancing COTS products
 - Triggering systems for demand-assigned communications
 - Video and image compression





Recommendations

- Aviation security enhancements can be achieved through a number of technologies including communications
- Need to conduct rigorous process to define communications and security systems engineering requirements
- Process will identify technology gaps
- Communications technology can serve a major role in the improvement of aviation safety